ZW
AF/

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, Colorado 80527-2400

PATENT APPLICATION

ATTORNEY DOCKET NO. 30003052-2

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor(s): Richard BROWN et al.

Confirmation No.: 7199

Application No.: 10/075,380

Examiner: Laurel L. Lashley

Filing Date: 2/15/2002

Group Art Unit: 2132

Title: IMPROVEMENTS IN AND RELATING TO DIGITAL CERTIFICATES

Mail Stop Appeal Brief-Patents
Commissioner For Patents
PO Box 1450
Alexandria, VA 22313-1450

TRANSMITTAL OF APPEAL BRIEF

Transmitted herewith is the Appeal Brief in this application with respect to the Notice of Appeal filed on May 24, 2006.

The fee for filing this Appeal Brief is (37 CFR 1.17(c)) $500.00.

(complete (a) or (b) as applicable)

The proceedings herein are for a patent application and the provisions of 37 CFR 1.136(a) apply.

□ (a) Applicant petitions for an extension of time under 37 CFR 1.136 (fees: 37 CFR 1.17(a)-(d)) for the total number of months checked below:

□ 1st Month $120 □ 2nd Month $450 □ 3rd Month $1020 □ 4th Month $1590

□ The extension fee has already been filed in this application.

☒ (b) Applicant believes that no extension of time is required. However, this conditional petition is being made to provide for the possibility that applicant has inadvertently overlooked the need for a petition and fee for extension of time.

Please charge to Deposit Account 08-2025 the sum of $ 500. At any time during the pendency of this application, please charge any fees required or credit any over payment to Deposit Account 08-2025 pursuant to 37 CFR 1.25. Additionally please charge any fees to Deposit Account 08-2025 under 37 CFR 1.16 through 1.21 inclusive, and any other sections in Title 37 of the Code of Federal Regulations that may regulate fees. A duplicate copy of this sheet is enclosed.

□ I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Commissioner for Patents, Alexandria, VA 22313-1450

Date of Deposit:

OR

□ I hereby certify that this paper is being transmitted to the Patent and Trademark Office facsimile number (571)273-8300.

Date of facsimile:

Typed Name:

Signature:

Respectfully submitted,

Richard BROWN et al.

By Reg. No. 43,438

for William T. Ellis

Attorney/Agent for Applicant(s)

Reg No. : 26,874

Date : June 28,2006

Telephone : 202-672-5300

Dkt. No. 30003052-2

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Applicant:	Richard BROWN et al.
Title:	IMPROVEMENTS IN AND RELATING TO DIGITAL CERTIFICATES
Appl. No.:	10/075,380
Filing Date:	2/15/2002
Examiner:	Laurel L. LASHLEY
Art Unit:	2132
Confirmation Number:	7199

BRIEF ON APPEAL

Mail Stop Appeal Brief - Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Under the provisions of 37 C.F.R. § 41.37, this Appeal Brief is being filed and authorization is hereby given to charge the $500.00 covering the 37 C.F.R. 41.20(b)(2) appeal fee and charge any deficiency (or credit any balance) to the undersigned deposit account 08-2025.

1. REAL PARTY IN INTEREST

The real party in interest is the assignee of record, Hewlett Packard Company.

2. RELATED APPEALS AND INTERFERENCES

There are no related appeals or interferences.

3. STATUS OF CLAIMS

Claims 1-22 are pending in the application. Claims 3 and 4 are objected to. Claims 1-2 and 5-22 are rejected and are the subject of this appeal.

4. STATUS OF AMENDMENTS

The present application is under a final rejection (See Final Rejection mailed February 24, 2006). Appeal of claims 1-2 and 5-22 is appropriate because all of these claims have been twice rejected. See 35 U.S.C. § 134(a). There are no amendments after final rejection.

5. SUMMARY OF CLAIMED SUBJECT MATTER

The invention of independent claim 1 is directed to a digital certificate (2) embodied on a computer readable medium executable on a computing system. The certificate (2) comprises a credential attribute function (6) associated with a credential attribute property (5) (FIG. 1, p. 7, lines 13-18). The credential attribute property (5) can have a plurality of values (12). The credential attribute function (6) is embedded in the digital certificate (2) as an executable program file (p. 7, lines 30-32), in which the credential attribute function (6) can determine the value (12) of the credential attribute property (5) at least partly when the executable program file is executed (p. 8, lines 17-24).

The invention of independent claim 18 is directed to a digital certificate (2) embodied on a computer readable medium executable on a computing system. The certificate (2) comprises a credential attribute function (6) with a credential attribute property (5) (FIG. 1, p. 7, lines 13-18). The credential attribute property (5) can have a plurality of values (12). The credential attribute function (6) is in the digital certificate (2) as an executable program file (p. 7, lines 30-32), in which the credential attribute function (6) can at least in part, when the executable program file is executed, determine the value (12) of the credential attribute property (5) (p. 8, lines 17-24).

The invention of independent claim 19 is directed to a digital certificate (2) embodied on a computer readable medium executable on a computing system. The certificate (2) comprises a credential attribute function (6) with a credential attribute property (5) (FIG. 1, p. 7, lines 13-18). The credential attribute property (5) can have a plurality of values (12). The credential attribute function (6) is in the digital certificate (2) as an executable program file (p. 7, lines 30-32), in which the credential attribute function (6) can at least in part, when the executable program file is executed, determine the value (12) of the credential attribute property (5) automatically (p. 8, lines 17-24, p. 11, lines 12-15).

6. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

The grounds of rejection to be reviewed on appeal are:

A. the rejection of claims 1, 5-14 and 18-19 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,189,097 to Tycksen ("Tycksen") in view of U.S. Patent No. 5,978,484 to Apperson et al. ("Apperson"); and

B. the rejection of claims 2, 15-17 and 20-22 under 35 U.S.C. § 103(a) as being unpatentable over Tycksen in view of U.S. Patent No. 5,659,616 to Sudia ("Sudia").

7. ARGUMENT

As an initial matter, appellants note that claims 1-22 stand provisionally rejected under the judicially created doctrine of obvious-type double patenting. This double patenting rejection is not subject to this appeal to the extent that appellants are willing to file a terminal disclaimer if the Examiner follows appropriate procedure as outlined in the MPEP.

Specifically, claims 1-22 stand provisionally rejected under the judicially created doctrine of obvious-type double patenting as being unpatentable over claims 1-38 of copending U.S. Patent Application No. 10/075,445 (hereafter "the '445 application"). Claims of the '445 application have been provisionally rejected under the judicially created doctrine of obvious-type double patenting as being unpatentable over claims of the present application. Accordingly, appellants respectfully request that the Examiner follow the procedure outlined in the MPEP and allow one of the present application and copending '445 application, at which time a Terminal Disclaimer will be filed in the other application if such is warranted. (See MPEP 822.01).

A. The rejection of claims 1, 5-14 and 18-19 under 35 U.S.C. § 103(a) as being unpatentable over Tycksen in view of Apperson

1. Claims 1, 5-14 and 18-19 of which claims 1, 18 and 19 are independent

Independent claim 1 is directed to a digital certificate, and recites "which credential attribute function is embedded in the digital certificate as an executable program file, in which the credential attribute function can determine the value of the credential attribute property at least partly when the executable program file is executed." Tycksen, Apperson, and Sudia fail to suggest at least this feature of claim 1.

Tycksen discloses a digital certificate 10 which is issued as proof of ownership to a digital product purchaser 14 of a given digital product 16 (See FIG. 2, col. 4, lines 37-41). The digital certificate 10 may include a number of components 11, which may be text-based or binary –based (See FIG. 1, col. 7, lines 27-48).

The Examiner is not clear on the position on whether or not Tycksen discloses a credential attribute function, as recited in claim 1, embedded within its digital certificate 10 as an executable program file. On page 3, first paragraph of the Final Office Action, the Examiner states that Tycksen "does not explicitly disclose a credential attribute function is embedded in the digital certificate as an executable program file, in which the credential attribute function can determine the value of the credential attribute property at least partly when the executable program file is executed", but on page 7, last paragraph states that Tycksen "does teaches the digital certificate having . . . a credential attribute function associated with the at least one credential attribute property, which function determines the value of the credential attribute property within the valid period." In any event, as appellants explain below, Tycksen does not include a credential attribute function, as recited in claim 1, embedded within its digital certificate 10 as an executable program file.

Tycksen does not include a credential attribute function, as recited in claim 1, embedded within its digital certificate 10 as an executable program file. While Tycksen discloses that its digital product 16 may be an executable computer program, or even a digital image, (See col. 4, lines 27-41, 46-49), the digital product 16 is separate from the digital certificate 10, and is not disclosed as functioning like the credential attribute function of claim 1. There is no suggestion in Tycksen of including a credential attribute function, as that credential attribute function is recited in claim 1, embedded within its digital certificate 10 as an executable program file.

Apperson also fails to disclose "which credential attribute function is embedded in the digital certificate as an executable program file, in which the credential attribute function can determine the value of the credential attribute property at least partly when the executable program file is executed" as recited in claim 1, and thus fails to cure the deficiencies of Tycksen. Apperson discloses an executable object 20 including executable code 30 and credentials 38 associated with a server computer or distributing authority (See FIG. 2, col. 4, lines 55-59). Apperson further discloses that the credentials may comprise a digital certificate (col. 8, lines 3-8). The executable code 30, however, is not embedded in the digital certificate of Apperson, as required by claim 1. Instead, both the executable code 30 and the digital certificate as part of the credentials 38, are part of the executable object 20.

Moreover, the executable code 30 of Apperson is not disclosed as determining the value of a credential attribute property. Thus, even if the executable code 30 is an executable program file, it does not "determine the value of the credential attribute property at least partly when the executable program file is executed" as required by claim 1. Thus, even if Tycksen and Apperson were combined, the result would not meet the features of claim 1.

With respect to Apperson, the Examiner equates the CA's certificate 71 of Apperson with the credential attribute function as claimed, and states on page 3 of the Final Office Action, "The Examiner believes the CA's certificate to be a credential attribute function because the certificate 'indicates an authorized set of privileges' which verifies levels of trustworthiness and executes code based on the level of trust identified." Nowhere, however, does Apperson disclose that the certificate 71 executes code, or that code embedded thereon is executed, much less to determine the value of the credential attribute property.

Independent claims 18 and 19 respectively recite "which credential attribute function is in the digital certificate as an executable program file, in which the credential attribute function can at least in part, when the executable program file is executed, determine the value of the credential attribute property", and "which credential attribute function is in the digital certificate as an executable program file, in which the credential attribute function can at least in part, when the executable program file is executed, determine the value of the credential attribute property automatically", and thus are patentable for reasons analogous to claim 1, as discussed earlier herein.

Dependent claims 5-14 all ultimately depend from independent claim 1, and are allowable for at least the same reasons, as well as for further patentable features recited therein.

B. The rejection of claims 2, 15-17 and 20-22 under 35 U.S.C. § 103(a) as being unpatentable over Tycksen in view of Sudia

1. Claims 2, 15-17 and 20-22, all of which ultimately depend from independent claim 1.

Sudia fails to disclose "which credential attribute function is embedded in the digital certificate as an executable program file, in which the credential attribute function can determine the value of the credential attribute property at least partly when the executable program file is executed" as recited in claim 1. The Examiner appears to recognized this deficiency in Sudia, stating on page 7 of the Final Office Action that Sudia "does not teach the digital certificate having a valid period, and a credential attribute function associated with the at least one credential attribute property, which function determines the value of the credential attribute property within the valid period." The Examiner supplies Tycksen for teaching the credential function. However, for the reasons discussed above with respect to the rejection of claim 1, Tycksen does not disclose "a credential attribute function is embedded in the digital certificate as an executable program file, in which the credential attribute function can determine the value of the credential attribute property at least partly when the executable program file is executed", and thus fails to cure the deficiencies of Sudia.

Dependent claims 2, 15-17 and 20-22 all ultimately depend from independent claim 1, and are allowable for at least the same reasons, as well as for further patentable features recited therein.

CONCLUSION

For the foregoing reasons, it is submitted that the PTO's rejections are erroneous, and reversal of the applied rejections is respectfully requested.

Respectfully submitted,

Date: June 28, 2006

HEWLETT-PACKARD COMPANY
Customer No.: 022879

By Thomas G. Bilodeau

William T. Ellis
Attorney for Applicant
Registration No. 26,874

Thomas G. Bilodeau
Attorney for Applicant
Registration No. 43,438

8. CLAIMS APPENDIX

1. (Previously Presented) A digital certificate embodied on a computer readable medium executable on a computing system, the certificate comprising:

a credential attribute function associated with a credential attribute property, which credential attribute property can have a plurality of values, which credential attribute function is embedded in the digital certificate as an executable program file, in which the credential attribute function can determine the value of the credential attribute property at least partly when the executable program file is executed.

2. (Previously Presented) A digital certificate according to claim 1, in which there is provided a digital certificate comprising a credential attribute and at least one credential attribute property, the digital certificate having a valid period, and a credential attribute function associated with at least one credential attribute property, which function determines the value of the credential attribute property within the valid period.

3. (Original) A digital certificate according to claim 1, in which the credential attribute function varies the credential attribute property value as a function of time.

4. (Original) A digital certificate according to claim 3, in which the credential attribute function is monotonically decreasing over time.

5. (Original) A digital certificate according to claim 1, in which the credential attribute function is configured to determine the credential attribute property value automatically.

6. (Previously Presented) A digital certificate according to claim 1, in which execution of the executable program file fully can determine the credential attribute property value.

7. (Previously Presented) A digital certificate according to claim 1, in which the executable program file is a platform portable code.

8. (Original) A digital certificate according to claim 1, in which the credential attribute property comprises a value operated on by the credential attribute function to determine a credential attribute property value.

9. (Original) A digital certificate according to claim 1, in which the credential attribute function uses data obtained from outside the digital certificate to determine the credential attribute property value.

10. (Original) A digital certificate according to claim 9, in which the data obtained is obtained from a user by the input of data in response to a query generated by the credential attribute function.

11. (Original) A digital certificate according to claim 9, in which the data obtained is obtained from a digital data store.

12. (Original) A digital certificate according to claim 11, in which the digital data store is a web site.

13. (Original) A digital certificate according to claim 1, in which there is a plurality of credential attributes in the digital certificate.

14. (Original) A digital certificate according to claim 1, in which there is a plurality of credential attribute properties in the digital certificate.

15. (Original) A digital certificate according to claim 14, in which a plurality of the credential attribute properties have respective attribute functions.

16. (Original) A digital certificate according to claim 15, in which each credential attribute property has a respective attribute function.

17. (Original) A digital certificate according to claim 1, in which the digital certificate has a valid period and the credential attribute function determines the value of the credential attribute property within the valid period.

18. (Previously Presented) A digital certificate embodied on a computer readable medium executable on a computing system, the certificate comprising:

a credential attribute function with a credential attribute property, which credential attribute property can have a plurality of values, which credential attribute function is in the digital certificate as an executable program file, in which the credential attribute function can at least in part, when the executable program file is executed, determine the value of the credential attribute property.

19. (Previously Presented) A digital certificate embodied on a computer readable medium executable on a computing system, the certificate comprising:

a credential attribute function with a credential attribute property, which credential attribute property can have a plurality of values, which credential attribute function is in the digital certificate as an executable program file, in which the credential attribute function can at least in part, when the executable program file is executed, determine the value of the credential attribute property automatically.

20. (Previously Presented) A method of communication, which method comprises the steps of communicating from a sender to a recipient a digital certificate according to claim 1.

21. (Original) A method of communication according to claim 20, in which the recipient inspects the digital certificate and the credential attribute property value is determined according to the credential attribute function.

22. (Original) A method of communication according to claim 20, in which the communication at least in part is via a distributed electronic network.

9. EVIDENCE APPENDIX

None.

10. RELATED PROCEEDINGS APPENDIX

None.